

# Minimum orbit dimension for local unitary action on $n$ -qubit pure states

David W. Lyons  
lyons@lvc.edu  
Mathematical Sciences  
Lebanon Valley College

Scott N. Walck  
walck@lvc.edu  
Department of Physics  
Lebanon Valley College

revised: 9 September 2005

**Abstract.** The group of local unitary transformations partitions the space of  $n$ -qubit quantum states into orbits, each of which is a differentiable manifold of some dimension. We prove that all orbits of the  $n$ -qubit quantum state space have dimension greater than or equal to  $3n/2$  for  $n$  even and greater than or equal to  $(3n+1)/2$  for  $n$  odd. This lower bound on orbit dimension is sharp, since  $n$ -qubit states composed of products of singlets achieve these lowest orbit dimensions.

## 1 Introduction

Quantum entanglement theory can be regarded as the branch of nonrelativistic quantum mechanics that seeks to understand the states and dynamics of composite quantum systems with a fixed number of subsystems. Composite quantum systems can exhibit correlations among subsystems in ways that classically describable composite systems cannot. A (pure) state of a composite quantum system is called entangled if it cannot be described by specifying (pure) states for each of the subsystems.

Quantum entanglement plays a particularly important role in quantum information, where the subsystems are quantum bits or qubits (a spin-1/2 particle is a physical realization of a qubit). An  $n$ -qubit system is the quantum analog of an  $n$ -bit computer or communications channel. Because quantum computing algorithms and quantum communications protocols utilize entanglement as an essential resource, potential applications of quantum information theory provide motivation for a more complete description of entanglement (see [1, 2] for surveys of a broad range of topics in this area).

A fundamental problem in the theory of quantum entanglement is to describe the types of entanglement that are achievable for a composite quantum system. We regard two states of a composite quantum system as having the same type of

entanglement if unitary operations on the subsystems, called local unitary or LU transformations, can transform one quantum state into the other. Local unitary transformations form a Lie group which acts on the manifold of quantum states, partitioning it into orbits. Each orbit is a differentiable manifold that represents a type of quantum entanglement. The *orbit space*—the set of orbits made into a topological space by the quotient topology—is the collection of entanglement types.

A theory of quantum entanglement based on local unitary transformations seeks to describe the orbit spaces and the orbits themselves for composite quantum systems. Much of the progress toward understanding the orbit spaces of quantum systems comes from invariant theory—the study of functions which are constant along orbits [3, 4, 5, 6, 7, 8, 9, 10, 11, 12]. One hopes to use these invariants, which are usually polynomial functions of state vector coefficients, to distinguish and classify orbits. Rains [3] and Grassl et al. [4] laid the groundwork for a systematic approach using this philosophy. The success in choosing particular, finite sets of invariants to label points in the orbit space has so far been limited to small numbers of qubits. Makhlin [6] gave a set of 18 polynomial invariants that separate orbits for two-qubit mixed states. Sudbery [5] gave a set of six polynomial invariants that separate orbits for 3-qubit pure states. Acín et al. [13, 14] gave a convenient set of non-polynomial invariants and a classification of 3-qubit pure states based on it.

In this paper we pursue a strategy inspired by Linden and Popescu [15, 16], who approached entanglement properties of quantum states working on the Lie algebra level to study the orbits themselves. We develop a general technique for calculating the orbit dimension of a state and use this to prove a lower bound on orbit dimension. We have also used our methods to provide a proof [17] of the authors’ claim in [15, 16] that almost all states have orbit dimension  $3n$  (we take the manifold of pure  $n$ -qubit states to be the projective space  $\mathbb{P}((\mathbb{C}^2)^{\otimes n})$  and the group of local unitary transformations to be  $G = \text{SU}(2)^n$ ).

Most of the progress in understanding orbits and orbit dimensions has been for systems of only for two or three qubits. Carteret and Sudbery [18] described the non-generic orbits (including orbit dimensions) for pure 3-qubit states. Życzkowski et al. [19, 20] analyze orbits for bipartite states. Few general results are known about those orbits which are the most interesting from the quantum information point of view, namely the non-generic or exceptional orbits of  $n$ -qubit states (basic examples are the singlet state of two qubits and the GHZ state of three qubits). The main result in the present paper is at least a small step towards the larger goal of orbit classification for general  $n$ .

## Physical Significance of the Result

In this paper, we identify the minimum orbit dimension of  $n$ -qubit quantum states. States that have the minimum orbit dimension are, in some sense, the “rarest” quantum states. Until now, it has been known that singlet states have

minimum orbit dimension for two qubits, and one could conjecture that some  $n$ -qubit generalization of the singlet state would have minimum orbit dimension for  $n$  qubits, but it was not clear how the singlet should be generalized to maintain the minimum orbit dimension as  $n$  increases. For example, one generalization of the singlet is the so-called  $n$ -cat state,  $(1/\sqrt{2})|00 \cdots 00\rangle + (1/\sqrt{2})|11 \cdots 11\rangle$ , of which the GHZ state is an example for three qubits. But the  $n$ -cat generalization of the singlet does not maintain the minimum orbit dimension for higher qubit numbers. As we show in this paper, it is the product of singlet states (for even qubit numbers) or the product of singlets and one unentangled qubit (for odd qubit numbers) that is the generalization of singlets that achieves minimum orbit dimension. This suggests a special role for the 2-qubit singlet state in the theory of  $n$ -qubit quantum entanglement.

## Proof Strategy and Outline

To establish the minimum orbit dimension, we show that the orbit dimension of a given state is (one less than) the rank of a real matrix  $M$  associated to that state. The matrix  $M$  arises naturally via consideration of the action of the local unitary group on an infinitesimal level, that is, the action of the Lie algebra of the local unitary group. The column vectors of  $M$  can be identified with complex vectors. We then establish lower bounds on the rank of  $M$  by showing that a sufficient number of real dot products of columns of  $M$  can be arranged, possibly after local unitary operations, to vanish. Instead of working directly with real dot products, it is convenient to calculate complex inner products; the vanishing of the real part of a complex inner product guarantees that the real dot product is zero (see (15) below).

In §3 we introduce the matrix  $M$ . To establish the necessary cancellations among terms of complex inner products of columns of  $M$  requires careful book-keeping and a technical lemma; we present this machinery in §4. Next we establish orthogonality among columns of  $M$  in §5 and §6. We then use these results to prove minimum orbit dimension in §7.

## 2 Conventions and notation

### Hilbert space, state space and the local unitary group

Let  $H = (\mathbb{C}^2)^{\otimes n}$  denote the Hilbert space of pure states of a system of  $n$  qubits and let  $\mathbb{P}(H)$  denote the projectivization of  $H$  which is the state space of the system. We take the local unitary group to be  $G = \text{SU}(2)^n$ . These definitions constitute a minor departure, made for the sake of clarity and compactness of exposition, from the widespread practice of taking state space to be the set of normalized state vectors and resolving phase ambiguity by including an extra  $\text{U}(1)$  factor in the local unitary group.

### Multi-index notation for Hilbert space basis vectors

Let  $|0\rangle, |1\rangle$  denote the standard basis for  $\mathbb{C}^2$  and write  $|i_1 i_2 \dots i_n\rangle$  for  $|i_1\rangle \otimes |i_2\rangle \otimes \dots \otimes |i_n\rangle$  in  $(\mathbb{C}^2)^{\otimes n}$ . For a multi-index  $I = (i_1 i_2 \dots i_n)$  with  $i_k = 0, 1$  for  $1 \leq k \leq n$ , we will write  $|I\rangle$  to denote  $|i_1 i_2 \dots i_n\rangle$ . Let  $i_k^c$  denote the bit complement

$$i_k^c = \begin{cases} 0 & \text{if } i_k = 1 \\ 1 & \text{if } i_k = 0 \end{cases}$$

and let  $I_k$  denote the multi-index

$$I_k := (i_1 i_2 \dots i_{k-1} i_k^c i_{k+1} \dots i_n)$$

obtained from  $I$  by taking the complement of the  $k$ th bit for  $1 \leq k \leq n$ . Similarly, let  $I_{kl}$  denote the multi-index

$$I_{kl} := (i_1 i_2 \dots i_{k-1} i_k^c i_{k+1} \dots i_{l-1} i_l^c i_{l+1} \dots i_n)$$

obtained from  $I$  by taking the complement of the  $k$ th and  $l$ th bits for  $1 \leq k < l \leq n$ .

### Standard identification of $\mathbb{C}^N$ with $\mathbb{R}^{2N}$

We identify the complex vectors in  $\mathbb{C}^N$  with real vectors in  $\mathbb{R}^{2N}$  via

$$\begin{aligned} \mathbb{C}^N &\leftrightarrow \mathbb{R}^{2N} \\ (z_1, z_2, \dots, z_N) &\leftrightarrow (a_1, b_1, a_2, b_2, \dots, a_N, b_N) \end{aligned} \quad (1)$$

where  $z_j = a_j + ib_j$  for  $1 \leq j \leq N$ .

## 3 Lie algebra action

The Lie algebra  $\mathfrak{su}(2)$  of  $\mathrm{SU}(2)$  is the set of traceless skew Hermitian matrices

$$\mathfrak{su}(2) = \left\{ \begin{bmatrix} it & u \\ -\bar{u} & -it \end{bmatrix} : t \in \mathbb{R}, u \in \mathbb{C} \right\}$$

and the Lie algebra  $LG = (\mathfrak{su}(2))^n$  of the local unitary group  $G = (\mathrm{SU}(2))^n$  is the set of  $n$ -tuples of matrices of this form.

A local unitary operator  $g = (g_1, g_2, \dots, g_n)$  in  $G$  acts on a product state vector  $|v\rangle = |v_1\rangle \otimes |v_2\rangle \otimes \dots \otimes |v_n\rangle$  in Hilbert space  $H = (\mathbb{C}^2)^{\otimes n}$  by

$$g \cdot |v\rangle = g_1 |v_1\rangle \otimes g_2 |v_2\rangle \otimes \dots \otimes g_n |v_n\rangle. \quad (2)$$

The induced action on  $|v\rangle$  by  $X = (X_1, X_2, \dots, X_n)$  in  $LG$  is given by

$$X \cdot |v\rangle = \sum_{i=1}^n |v_1\rangle \otimes \dots \otimes |v_{i-1}\rangle \otimes X_i |v_i\rangle \otimes |v_{i+1}\rangle \otimes \dots \otimes |v_n\rangle. \quad (3)$$

This action extends linearly to all of Hilbert space as follows. Let  $|\psi\rangle = \sum_I c_I |I\rangle$  be an element in Hilbert space  $H$ , and let  $X = (X_1, X_2, \dots, X_n)$  be an element of  $LG$  with

$$X_k = \begin{bmatrix} it_k & u_k \\ -\overline{u_k} & -it_k \end{bmatrix} \quad \text{for } 1 \leq k \leq n.$$

A straightforward calculation shows that the action of  $X$  on  $|\psi\rangle$  is given by

$$X \cdot |\psi\rangle = \sum_I \left( \sum_{k=1}^n (-1)^{i_k} [c_I it_k + c_{I_k} \text{conj}^{i_k}(u_k)] \right) |I\rangle \quad (4)$$

where  $\text{conj}^1(z) = \overline{z}$  and  $\text{conj}^0(z) = z$ . Let  $a_I, b_I$  denote the real and imaginary parts of the coefficient  $c_I$  in the expression for  $|\psi\rangle$ , and let  $r_k, s_k$  denote the real and imaginary parts of the entry  $u_k$  in  $X_k$ . The real and imaginary parts of the  $I$ th coefficient on the right hand side of equation (4) are the following.

$$\text{Re}\langle I|X|\psi\rangle = \sum_{k=1}^n [(-1)^{i_k}(-b_I t_k) + (-1)^{i_k} a_{I_k} r_k - b_{I_k} s_k] \quad (5)$$

$$\text{Im}\langle I|X|\psi\rangle = \sum_{k=1}^n [(-1)^{i_k}(a_I t_k) + (-1)^{i_k} b_{I_k} r_k + a_{I_k} s_k] \quad (6)$$

Given a state  $x$  in  $\mathbb{P}(H)$ , the isotropy Lie subalgebra  $LI_x$  of the isotropy subgroup  $I_x$  is determined by the following condition.

**Proposition 3.1.** *Isotropy Lie algebra condition: Let  $x \in \mathbb{P}(H)$  be a state and let  $|\psi\rangle$  be a Hilbert space representative for  $x$ . The element  $X \in LG$  is in the Lie algebra  $LI_x$  of the isotropy subgroup  $I_x$  of  $x$  if and only if*

$$X \cdot |\psi\rangle = i\theta |\psi\rangle$$

for some real  $\theta$ .

With (5) and (6), Proposition 3.1 implies the following.

**Corollary 3.2.** *Let  $X, x$  and  $|\psi\rangle$  be as above. Suppose that  $X$  is in  $LI_x$ . Then for each multi-index  $I$ , we have the following pair of equations.*

$$\sum_{k=1}^n [(-1)^{i_k}(-b_I t_k) + (-1)^{i_k} a_{I_k} r_k - b_{I_k} s_k] = -b_I \theta \quad (7)$$

$$\sum_{k=1}^n [(-1)^{i_k}(a_I t_k) + (-1)^{i_k} b_{I_k} r_k + a_{I_k} s_k] = a_I \theta \quad (8)$$

for some real number  $\theta$ .

By adding  $b_I \theta$ , respectively  $-a_I \theta$ , to both sides of equation (7), respectively (8), the corollary shows that calculating the Lie algebra  $LI_x$  is a matter

of solving a homogeneous real linear system of  $2^{n+1}$  equations (two for each of the  $2^n$  multi-indices) in the  $3n + 1$  unknowns  $t_k, r_k, s_k, \theta$ . Let

$$M(t_1, r_1, s_1, t_2, r_2, s_2, \dots, t_n, r_n, s_n, \theta) = 0 \quad (9)$$

denote the linear system of  $2^{n+1}$  equations given by (7) and (8), so that the  $2^{n+1} \times (3n + 1)$  matrix for  $M$  has all entries of the form  $\pm a_I, \pm b_I$ .

Here is the fundamental observation which reduces the problem of orbit dimension to finding the rank of  $M$ .

**Proposition 3.3.** *Orbit dimension as rank of  $M$ : Let  $x$  be a state, let  $|\psi\rangle$  be a Hilbert space representative for  $x$ , and let  $M$  be the associated matrix constructed from the coordinates of  $|\psi\rangle$  as described above. Then we have*

$$\text{rank } M = \dim \mathcal{O}_x + 1.$$

PROOF. We can think of  $M$  as the matrix of a linear map  $M: LG \times \mathbb{R} \rightarrow \mathbb{R}^{2^{n+1}}$  via the identification

$$\begin{aligned} \mathbb{R}^{3n} &\leftrightarrow LG \\ (t_1, r_1, s_1, t_2, r_2, s_2, \dots, t_n, r_n, s_n) &\leftrightarrow (X_1, X_2, \dots, X_n) \end{aligned}$$

where  $X_k = \begin{bmatrix} it_k & r_k + is_k \\ -r_k + is_k & -it_k \end{bmatrix}$ . Consider a solution  $(X, \theta)$  of  $M(X, \theta) = 0$ . Proposition 3.1 says that  $|\psi\rangle$  is an eigenvector for  $X$  with eigenvalue  $i\theta$ , so  $\theta$  is determined by  $X$ . Since  $X \in LI_x$  if and only if  $M(X, \theta) = 0$  for some  $\theta$ , it follows that  $\dim LI_x = \dim \ker M$ . From this we have

$$\begin{aligned} \dim LI_x &= \dim \ker M \\ &= \text{number of columns of } M - \text{rank } M \\ &= 3n + 1 - \text{rank } M. \end{aligned}$$

Thus we have  $\dim \mathcal{O}_x = \dim G - \dim LI_x = 3n - (3n + 1 - \text{rank } M) = \text{rank } M - 1$ .  $\square$

Next we introduce three operators on  $H$  whose purpose is to simplify calculations (specifically, inner products of column vectors) to establish the rank of  $M$ .

Let  $A = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ ,  $B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ , and  $C = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$  denote the standard<sup>1</sup> basis for  $\mathfrak{su}(2)$ , so that the element  $X = \begin{bmatrix} it & r + is \\ -r + is & -it \end{bmatrix}$  is written  $X = tA + rB + sC$  with respect to this basis.

<sup>1</sup>This basis is standard in the sense that  $A, B, C$  correspond to the truly standard basis vectors  $\mathbf{i} = (0, 1, 0, 0)$ ,  $\mathbf{j} = (0, 0, 1, 0)$ ,  $\mathbf{k} = (0, 0, 0, 1)$  of the pure quaternions, under the natural identification  $\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \leftrightarrow a + bj$ . In terms of the Pauli spin matrices, we have  $A = i\sigma_z$ ,

$B = i\sigma_y$  and  $C = i\sigma_x$  where  $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ ,  $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ , and  $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ .

Define elements  $A_k, B_k, C_k$  of  $LG$  for  $1 \leq k \leq n$  to have  $A, B, C$ , respectively, in the  $k$ th coordinate and zero elsewhere.

$$A_k = (0, \dots, 0, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, 0, \dots, 0)$$

$$B_k = (0, \dots, 0, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, 0, \dots, 0)$$

$$C_k = (0, \dots, 0, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, 0, \dots, 0)$$

Applying (4), we have the following.

$$A_k |\psi\rangle = \sum_I i(-1)^{i_k c_I} |I\rangle \quad (10)$$

$$B_k |\psi\rangle = \sum_I (-1)^{i_k c_{I_k}} |I\rangle \quad (11)$$

$$C_k |\psi\rangle = \sum_I i c_{I_k} |I\rangle \quad (12)$$

Simple checking shows that the complex vectors on the right hand sides of the above three equations identify with columns of  $M$  via the standard identification (1). The rightmost column of  $M$  identifies with  $-i |\psi\rangle$ . Thus we may view  $M$  as the  $(3n+1)$ -tuple of complex vectors

$$M = (A_1 |\psi\rangle, B_1 |\psi\rangle, C_1 |\psi\rangle, \dots, A_n |\psi\rangle, B_n |\psi\rangle, C_n |\psi\rangle, -i |\psi\rangle). \quad (13)$$

It is convenient to gather the columns of  $M$  into 3-tuples. We define the *triple*  $T_k$  to be the set of vectors

$$T_k = \{A_k |\psi\rangle, B_k |\psi\rangle, C_k |\psi\rangle\} \quad (14)$$

for  $1 \leq k \leq n$ . We view the vectors both as real and also as complex via (1).

## 4 Technical lemmas

In this section we present combinatorial machinery that will be used to establish orthogonality among columns of the matrix  $M$  described in the previous section.

**Lemma 4.1.** *Let  $L = (i_{jk})$  be an  $\ell \times m$  matrix with entries in  $\mathbb{Z}_2 = \{0, 1\}$ , and let  $E = ((-1)^{i_{jk}})$ . We view  $L$  as the matrix of a  $\mathbb{Z}_2$ -linear map  $\mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^\ell$  and we view  $E$  as the matrix of an  $\mathbb{R}$ -linear map. Suppose that  $E$  has a nontrivial kernel. Then either  $L$  has a nontrivial kernel or there is some  $v \in \mathbb{Z}_2^m$  such that  $Lv = (1, 1, \dots, 1)$ .*

**PROOF.** Assume the hypotheses of the lemma. Let  $N$  be the  $\ell \times m$  matrix whose entries are all ones. As matrices over  $\mathbb{R}$ , observe that  $E = N - 2L$ .

Since  $E$  has integer coefficients, there is a nonzero kernel vector  $v$  with integer coordinates. Dividing by a power of 2, if necessary, we may rescale  $v$  so that the integer coordinates are not all even. We have  $0 = Ev = (N - 2L)v$ , so  $Lv = (N/2)v = (s/2)c$ , where  $c$  is the column vector of all ones and  $s$  is the sum of the entries in  $v$ . Since  $Lv$  is a vector with integer entries,  $Lv = (s/2)c$  implies  $s$  is even. Now we can read the equation  $Lv = (s/2)c \pmod{2}$ . If  $s/2 = 0 \pmod{2}$ , then  $v \pmod{2}$  is a nonzero kernel vector for  $L$  since not all coordinates of  $v$  are even. If  $s/2 = 1 \pmod{2}$ , then  $c = (1, 1, \dots, 1)$  is in the image of  $L$ .  $\square$

**Corollary 4.2.** *Let  $\xi_1, \xi_2, \dots, \xi_m$  be real numbers, not necessarily distinct, and not all of which are zero. Let  $D_m$  be the  $2^m \times 2^m$  diagonal matrix whose  $r, r$  entry is*

$$\sum_{i=1}^m (-1)^{r_i} \xi_i$$

where  $r = (r_m r_{m-1} \dots r_2 r_1)$  is the binary expansion of the integer  $r$  in the range  $0 \leq r \leq 2^m - 1$ . Suppose that  $D_m$  has at least one zero eigenvalue. Let  $r^1, r^2, \dots, r^\ell$  be the row numbers of the zero eigenvalues of  $D_m$ . Then there is a nonempty set  $\mathcal{K} = \{k_1, k_2, \dots, k_{m'}\}$  with  $1 \leq k_1 < k_2 < \dots < k_{m'} \leq m$  and  $m'$  even so that

$$\sum_{k \in \mathcal{K}} r_k^1 = \sum_{k \in \mathcal{K}} r_k^2 = \dots = \sum_{k \in \mathcal{K}} r_k^\ell$$

where the sums are taken mod 2.

PROOF. Let  $L = (r_j^i)$  and let  $E = ((-1)^{r_j^i})$ . Since  $E$  kills the nonzero vector  $(\xi_1, \xi_2, \dots, \xi_m)$ , Lemma 4.1 applies. If  $L$  is not injective, let  $v = (v_1, v_2, \dots, v_m)$  be a nonzero kernel vector and let  $k_1, k_2, \dots, k_{m'}$  be the indices  $i$  in the range from 1 to  $m$  inclusive for which  $v_i = 1$ . Then the mod 2 equation  $Lv = 0$  yields

$$0 = \sum_{k \in \mathcal{K}} r_k^1 = \sum_{k \in \mathcal{K}} r_k^2 = \dots = \sum_{k \in \mathcal{K}} r_k^\ell.$$

If there is a  $v = (v_1, v_2, \dots, v_m)$  such that  $Lv = (1, 1, \dots, 1)$ , then setting  $k_1, k_2, \dots, k_{m'}$  to be the indices  $i$  for which  $v_i = 1$ , then we have

$$1 = \sum_{k \in \mathcal{K}} r_k^1 = \sum_{k \in \mathcal{K}} r_k^2 = \dots = \sum_{k \in \mathcal{K}} r_k^\ell.$$

To see that  $m'$  must be even, note that if

$$0 = \sum_{i=1}^m (-1)^{r_i} \xi_i$$

then we also have

$$0 = - \sum_{i=1}^m (-1)^{r_i} \xi_i = \sum_{i=1}^m (-1)^{r_i^c} \xi_i.$$

So if  $r^1 = r$  is a row number for a zero entry in  $D_m$ , so is  $r^2 = r^c$ , where  $r^c$  is the binary string obtained from  $r$  by complementing each bit. Since these two



rows have opposite parity in each bit,  $m'$  cannot be odd. This completes the proof.  $\square$

**Definition 4.3.** For the set  $\mathcal{K} = \{k_1, k_2, \dots, k_{m'}\}$  arising from zero entries in  $D_m$  in row numbers  $r^1, r^2, \dots, r^l$  as in 4.2 above, we define the *parity of  $\mathcal{K}$*  to be the common value in  $\mathbb{Z}_2$  of the sums

$$\sum_{k \in \mathcal{K}} r_k^1 = \sum_{k \in \mathcal{K}} r_k^2 = \dots = \sum_{k \in \mathcal{K}} r_k^\ell.$$

Now we are ready to establish lower bounds on the rank of  $M$  by showing that inner products of certain pairs of columns can be arranged (via local unitary equivalence operations) to vanish.

## 5 Orthogonality Results

Throughout this section, let  $|\psi\rangle = \sum_I c_I |I\rangle \in H$  be a Hilbert space vector, and let  $M$  be the associated matrix as defined in §3.

We make repeated use of the following elementary observation about the relationship between complex and real inner products. Let  $u, v$  be vectors in  $\mathbb{C}^N$  and let  $u', v'$  be the corresponding vectors in  $\mathbb{R}^{2N}$  given by the standard identification (1). The complex inner product  $\langle u | v \rangle$  and the real dot product  $u' \cdot v'$  are related by

$$\operatorname{Re}(\langle u | v \rangle) = u' \cdot v'. \quad (15)$$

We shall consider complex inner products given in Table 1 among the column vectors<sup>2</sup> of  $M$  given in (13).

Our first proposition is that each triple spans three real dimensions.

**Proposition 5.1.** *Let  $T_k = \{A_k |\psi\rangle, B_k |\psi\rangle, C_k |\psi\rangle\}$  be a triple of columns of  $M$ . The three vectors in the triple are orthogonal when viewed as real vectors.*

**PROOF.** To prove the proposition, we show that inner products (F), (J), and (K) in Table 1 are pure imaginary for the case  $j = k$ . First, for (F), the  $I$ th summand is

$$-i(-1)^{i_k+i_k} \overline{c_I} c_{I_k} = -i \overline{c_I} c_{I_k}$$

and the  $I_k$ th summand is

$$-i(-1)^{i_k+1+i_k+1} \overline{c_{I_k}} c_I = -i \overline{c_{I_k}} c_I.$$

The sum of the  $I$ th and the  $I_k$ th summands is therefore  $-2i \operatorname{Re}(\overline{c_I} c_{I_k})$ . By pairing the summands in this way, we see that  $\langle \psi | A_k^\dagger B_k |\psi \rangle$  is pure imaginary. Thus it follows from (15) that  $A_k |\psi\rangle, B_k |\psi\rangle$  are orthogonal as real vectors.

<sup>2</sup>For the sake of compactness we have omitted a factor of  $-i$  in the inner products (A), (E), and (I). With or without the factor  $-i$ , their vanishing guarantees the orthogonality of the rightmost column vector  $-i|\psi\rangle$  of  $M$  to  $A_k |\psi\rangle, B_k |\psi\rangle$ , and  $C_k |\psi\rangle$ .

$$\langle \psi | A_k | \psi \rangle = \sum_I i(-1)^{i_k} |c_I|^2 \quad (\text{A})$$

$$\langle \psi | A_j^\dagger A_k | \psi \rangle = \sum_I (-1)^{i_j+i_k} |c_I|^2 \quad (\text{B})$$

$$\langle \psi | B_j^\dagger A_k | \psi \rangle = \sum_I i(-1)^{i_j+i_k} \overline{c_{I_j}} c_I \quad (\text{C})$$

$$\langle \psi | C_j^\dagger A_k | \psi \rangle = \sum_I (-1)^{i_k} \overline{c_{I_j}} c_I \quad (\text{D})$$

$$\langle \psi | B_k | \psi \rangle = \sum_I (-1)^{i_k} \overline{c_I} c_{I_k} \quad (\text{E})$$

$$\langle \psi | A_j^\dagger B_k | \psi \rangle = \sum_I -i(-1)^{i_j+i_k} \overline{c_I} c_{I_k} \quad (\text{F})$$

$$\langle \psi | B_j^\dagger B_k | \psi \rangle = \sum_I (-1)^{i_j+i_k} \overline{c_{I_j}} c_{I_k} \quad (\text{G})$$

$$\langle \psi | C_j^\dagger B_k | \psi \rangle = \sum_I -i(-1)^{i_j} \overline{c_{I_j}} c_{I_k} \quad (\text{H})$$

$$\langle \psi | C_k | \psi \rangle = \sum_I i \overline{c_I} c_{I_k} \quad (\text{I})$$

$$\langle \psi | A_j^\dagger C_k | \psi \rangle = \sum_I (-1)^{i_j} \overline{c_I} c_{I_k} \quad (\text{J})$$

$$\langle \psi | B_j^\dagger C_k | \psi \rangle = \sum_I i(-1)^{i_j} \overline{c_{I_j}} c_{I_k} \quad (\text{K})$$

$$\langle \psi | C_j^\dagger C_k | \psi \rangle = \sum_I \overline{c_{I_j}} c_{I_k} \quad (\text{L})$$

Table 1: Inner products of pairs of columns of  $M$

Next we consider (J) with  $j = k$ . The  $I$ th summand is  $(-1)^{i_k} \overline{c_I} c_{I_k}$ , while the  $I_k$ th summand is  $(-1)^{i_k+1} \overline{c_{I_k}} c_I$ . Thus the sum of the  $I$ th and  $I_k$ th summands is  $(-1)^{i_k} 2i \text{Im}(\overline{c_I} c_{I_k})$ , which is pure imaginary, so  $A_k |\psi\rangle, C_k |\psi\rangle$  are orthogonal as real vectors.

Finally we check (K) for  $j = k$ . In this case the  $I$ th summand is  $i(-1)^{i_k} |c_{I_k}|^2$  so the inner product is pure imaginary. Therefore  $B_k |\psi\rangle, C_k |\psi\rangle$  are orthogonal as real vectors. This establishes the proposition.  $\square$

Next we show that a nontrivial linear dependence among the columns  $A_k |\psi\rangle$  as real vectors guarantees that certain columns among the  $B_k |\psi\rangle, C_k |\psi\rangle$  are orthogonal to spans of certain sets of triples.

**Proposition 5.2.** *Main orthogonality proposition: Suppose that*

$$\sum_{k=1}^m \xi_k A_{j_k} |\psi\rangle = 0$$

for some  $1 \leq j_1 < j_2 < \dots < j_m \leq n$ ,  $\xi_j$  real and not all zero. Then there is a nonempty subset  $K \subseteq \{j_1, j_2, \dots, j_m\}$  containing an even number of elements such that  $B_k |\psi\rangle$  and  $C_k |\psi\rangle$  are orthogonal to  $-i |\psi\rangle$  and to  $A_j |\psi\rangle, B_j |\psi\rangle, C_j |\psi\rangle$  for all  $k \in K, j \notin K$ .

PROOF. Let  $D_m$  be the matrix constructed from  $\xi_1, \dots, \xi_m$  as described in the technical lemmas section. Let  $c_I$  be a nonzero state vector coefficient. By (10), the  $I$ th coordinate of  $\sum_{k=1}^m \xi_k A_{j_k} |\psi\rangle$  is  $i c_I \sum_k (-1)^{i_{j_k}} \xi_k$ , so the hypothesis  $\sum_{k=1}^m \xi_k A_{j_k} |\psi\rangle = 0$  guarantees that  $D_m$  has at least one zero eigenvalue, namely  $\sum_k (-1)^{i_{j_k}} \xi_k$  where  $I$  is any multi-index for which  $c_I \neq 0$ . Therefore  $\xi_1, \xi_2, \dots, \xi_m$  and  $D_m$  meet the hypothesis of Corollary 4.2.

Let  $\mathcal{K} = \{k_1, k_2, \dots, k_{m'}\}$  be the subset of  $\{1, 2, \dots, m\}$  whose existence is guaranteed by 4.2 with corresponding parity  $b$  as defined in 4.3, and let  $K = \{j_{k_1}, j_{k_2}, \dots, j_{k_{m'}}\}$ . The set of multi-indices of state basis vectors  $|I\rangle$  is partitioned by  $K$  into two equal-sized equivalence classes by the following equivalence relation.

$$(i_1, i_2, \dots, i_n) \sim (i'_1, i'_2, \dots, i'_n) \Leftrightarrow \sum_{k \in K} i_k = \sum_{k \in K} i'_k \pmod{2} \quad (16)$$

In words,  $I \sim I'$  if the parity of the sum of bits in columns in  $K$  is the same for  $I$  and  $I'$ . Let  $\mathcal{P}$  be the set of multi-indices of parity class  $b$  and let  $\mathcal{P}'$  be the opposite parity class.

We claim that all complex inner products of the form (E)–(L) in Table 1 vanish for  $k \in K$  and  $j \notin K$ . From this it follows from (15) that the corresponding real dot products also vanish. Observe that for any  $I$  for which  $c_I \neq 0$  we have

$\sum_k (-1)^{i_{j_k}} \xi_k = 0$ , so  $I$  is in parity class  $\mathcal{P}$ . So if  $I, J$  are multi-indices in opposite parity classes, at least one of  $c_I, c_J$  must be zero. If  $k \in K$  and  $j \notin K$  then multi-indices  $I, I_k$  are in opposite parity classes, and also  $I_j, I_k$  are in opposite parity classes. Since every summand in each of the inner products (E)–(L) has a factor either of the form  $\overline{c_I} c_{I_k}$  or of the form  $\overline{c_{I_j}} c_{I_k}$  with  $k \in K$  and  $j \notin K$ , all of the inner products vanish.

This completes the proof.  $\square$

**Proposition 5.3.** *Suppose that for some  $1 \leq l < l' \leq n$  we have  $A_l |\psi\rangle = A_{l'} |\psi\rangle$  and  $C_l |\psi\rangle = C_{l'} |\psi\rangle$ . Then  $A_k |\psi\rangle, B_k |\psi\rangle$ , and  $C_k |\psi\rangle$  are each orthogonal to  $-i |\psi\rangle$  and to  $A_j |\psi\rangle, B_j |\psi\rangle, C_j |\psi\rangle$  for all  $k \in \{l, l'\}, j \notin \{l, l'\}$ .*

PROOF. We claim that all of the complex (and hence also real, by (15)) inner products (A)–(L) vanish for  $k \in \{l, l'\}$  and  $j \notin \{l, l'\}$ . We begin by applying Proposition 5.2 to the hypothesis  $A_l |\psi\rangle = A_{l'} |\psi\rangle$ . In the notation of 5.2 we have  $m = 2$  and therefore also  $m' = 2$  since  $m'$  is an even number in the range  $0 < m' \leq m$ , so  $K = \{l, l'\}$ . Thus we have from 5.2 that  $B_k |\psi\rangle$  and  $C_k |\psi\rangle$  are orthogonal to  $-i |\psi\rangle$  and to  $A_j |\psi\rangle, B_j |\psi\rangle, C_j |\psi\rangle$  for all  $k \in \{l, l'\}, j \notin \{l, l'\}$ .

It remains to be shown that  $A_l |\psi\rangle, A_{l'} |\psi\rangle$  are also orthogonal to  $-i |\psi\rangle$  and to  $A_j |\psi\rangle, B_j |\psi\rangle, C_j |\psi\rangle$  for all  $j \notin \{l, l'\}$ .

The hypothesis  $C_l |\psi\rangle = C_{l'} |\psi\rangle$  implies that  $c_{I_l} = c_{I_{l'}}$ , or equivalently, that  $c_I = c_{I_{l'}}$  for all  $I$ . This implies that summands of the inner products (A)–(D) cancel in pairs for  $k \in \{l, l'\}, j \notin \{l, l'\}$ , as follows. The  $I$ th summand of (A) is  $i(-1)^{i_k} |c_I|^2$  and the  $I_{l'}$ th summand is  $i(-1)^{i_k+1} |c_I|^2$ . The  $I$ th summand of (B) is  $(-1)^{i_j+i_k} |c_I|^2$  and the  $I_{l'}$ th summand is  $(-1)^{i_j+i_k+1} |c_I|^2$ . The  $I$ th summand of (C) is  $i(-1)^{i_j+i_k} \overline{c_{I_j}} c_I$  and the  $I_{l'}$ th summand is  $i(-1)^{i_j+i_k+1} \overline{c_{I_j}} c_I$ . The  $I$ th summand of (D) is  $(-1)^{i_k} \overline{c_{I_j}} c_I$  and the  $I_{l'}$ th summand is  $(-1)^{i_k+1} \overline{c_{I_j}} c_I$ .

This completes the proof.  $\square$

## 6 Local unitary adjustment

In this section we adapt the orthogonality results of the previous section to hypotheses involving more general linear dependencies.

Let us write  $\langle T_{i_1}, T_{i_2}, \dots, T_{i_r} \rangle$  to denote the subspace of the (real) column space of  $M$  spanned by the vectors in the triples  $T_{i_1}, \dots, T_{i_r}$  viewed as real vectors.

**Proposition 6.1.** *Main orthogonality proposition generalized: Suppose that*

$$\dim \langle T_{j_1}, T_{j_2}, \dots, T_{j_m} \rangle < 3m$$

*for some  $1 \leq j_1 < j_2 < \dots < j_m \leq n$ . Then there is a nonempty subset  $K \subseteq \{j_1, j_2, \dots, j_m\}$  containing an even number of elements such that there are*

two orthogonal vectors  $|\zeta_k\rangle, |\eta_k\rangle$  in  $\langle T_k \rangle$ , both of which are orthogonal to  $-i|\psi\rangle$ ,  $A_j|\psi\rangle$ ,  $B_j|\psi\rangle$  and to  $C_j|\psi\rangle$  for all  $k \in K, j \notin K$ .

PROOF. Let us write the linear dependency as a relation

$$\sum_{i=1}^m \xi_i |\phi_i\rangle = 0$$

where  $\xi_i$  is real,  $|\phi_i\rangle$  lies in  $\langle T_{j_i} \rangle$ ,  $\langle \phi_i | \phi_i \rangle = \langle \psi | \psi \rangle$  for  $1 \leq i \leq m$ , and not all the  $\xi_i$  are zero. Write each  $|\phi_i\rangle$  as a linear combination

$$|\phi_i\rangle = \alpha_i A_{j_i} |\psi\rangle + \beta_i B_{j_i} |\psi\rangle + \gamma_i C_{j_i} |\psi\rangle$$

with  $\alpha_i, \beta_i$  and  $\gamma_i$  real. Let  $R_i \in \text{SO}(\mathfrak{su}(2))$  be such that

$$R_i(A) = \alpha_i A + \beta_i B + \gamma_i C.$$

Since the adjoint representation  $\text{Ad}: \text{SU}(2) \rightarrow \text{SO}(\mathfrak{su}(2))$  is surjective, we can choose  $U_{j_i} \in \text{SU}(2)$  such that  $\text{Ad}(U_{j_i}^\dagger) = R_i$ , that is,  $U_{j_i}^\dagger X U_{j_i} = R_i X$  for all  $X \in \mathfrak{su}(2)$ . For  $j \notin \{j_1, j_2, \dots, j_m\}$ , set  $U_j$  equal to the identity. Finally, let  $U \in G = \text{SU}(2)^n$  be  $U = \prod_{i=1}^n U_i$ .

Now observe that

$$\sum_{i=1}^m \xi_i (U^\dagger A_{j_i} U) |\psi\rangle = \sum_{i=1}^m \xi_i |\phi_i\rangle = 0.$$

Applying  $U$  to both sides, we get

$$\sum_{i=1}^m \xi_i A_{j_i} (U |\psi\rangle) = 0.$$

Let  $M'$  be the matrix for the state vector  $U |\psi\rangle$ . Applying the main orthogonality proposition 5.2 to  $M'$ , we get that  $B_k(U |\psi\rangle), C_k(U |\psi\rangle)$  are orthogonal to  $U |\psi\rangle$  and to  $A_j U |\psi\rangle, B_j U |\psi\rangle, C_j U |\psi\rangle$  for  $k \in K, j \notin K$ . Now set

$$\begin{aligned} |\zeta_k\rangle &= U^\dagger B_k U |\psi\rangle \\ |\eta_k\rangle &= U^\dagger C_k U |\psi\rangle \end{aligned}$$

for  $k \in K$ . Since  $U$  is unitary, we have that  $|\zeta_k\rangle, |\eta_k\rangle$  are orthogonal to  $U^\dagger U |\psi\rangle = |\psi\rangle$  and to  $U^\dagger A_j U |\psi\rangle, U^\dagger B_j U |\psi\rangle, U^\dagger C_j U |\psi\rangle$  for  $k \in K, j \notin K$ . Since the three vectors  $U^\dagger A_j U |\psi\rangle, U^\dagger B_j U |\psi\rangle, U^\dagger C_j U |\psi\rangle$  have the same span as  $A_j |\psi\rangle, B_j |\psi\rangle, C_j |\psi\rangle$  for all  $j$ , the proposition is established.  $\square$

**Proposition 6.2.** *Generalization of 5.3: Suppose that  $\dim \langle T_l, T_{l'} \rangle \leq 4$  for some  $1 \leq l < l' \leq n$ . Then  $A_k |\psi\rangle, B_k |\psi\rangle$ , and  $C_k |\psi\rangle$  are each orthogonal to  $-i|\psi\rangle$  and to  $A_j |\psi\rangle, B_j |\psi\rangle, C_j |\psi\rangle$  for all  $k \in \{l, l'\}, j \notin \{l, l'\}$ .*

PROOF. The proof is very similar to the proof of 6.1.

Since  $\dim\langle T_l, T_{l'} \rangle \leq 4$ , the dimension of the intersection  $\langle T_l \rangle \cap \langle T_{l'} \rangle$  is at least two. Choose orthogonal vectors  $|\phi\rangle, |\phi'\rangle$  in  $\langle T_l \rangle \cap \langle T_{l'} \rangle$  with  $\langle \phi | \phi \rangle = \langle \phi' | \phi' \rangle = \langle \psi | \psi \rangle$ . Write linear combinations

$$\begin{aligned} |\phi\rangle &= \alpha_k A_k |\psi\rangle + \beta_k B_k |\psi\rangle + \gamma_k C_k |\psi\rangle \\ |\phi'\rangle &= \alpha'_k A_k |\psi\rangle + \beta'_k B_k |\psi\rangle + \gamma'_k C_k |\psi\rangle \end{aligned}$$

and let  $R_k \in \text{SO}(\text{su}(2))$  be such that

$$\begin{aligned} R_k(A) &= \alpha_k A + \beta_k B + \gamma_k C \\ R_k(C) &= \alpha'_k A + \beta'_k B + \gamma'_k C \end{aligned}$$

for  $k \in \{l, l'\}$ .

Since the adjoint representation  $\text{Ad}: \text{SU}(2) \rightarrow \text{SO}(\text{su}(2))$  is surjective, we can choose  $U_k \in \text{SU}(2)$  such that  $\text{Ad}(U_k^\dagger) = R_k$ , that is,  $U_k^\dagger X U_k = R_k X$  for all  $X \in \text{su}(2)$ . For  $j \notin \{l, l'\}$ , set  $U_j$  equal to the identity. Finally, let  $U \in G = \text{SU}(2)^n$  be  $U = \prod_{i=1}^n U_i$ .

Now observe that

$$\begin{aligned} U^\dagger A_l U |\psi\rangle &= |\phi\rangle = U^\dagger A_{l'} U |\psi\rangle \\ U^\dagger C_l U |\psi\rangle &= |\phi'\rangle = U^\dagger C_{l'} U |\psi\rangle \end{aligned}$$

Applying  $U$  to both sides, we get

$$\begin{aligned} A_l U |\psi\rangle &= A_{l'} U |\psi\rangle \\ C_l U |\psi\rangle &= C_{l'} U |\psi\rangle \end{aligned}$$

Let  $M'$  be the matrix for the state vector  $U |\psi\rangle$ . Applying 5.3 to  $M'$ , we get that  $A_k(U |\psi\rangle), B_k(U |\psi\rangle), C_k(U |\psi\rangle)$  are orthogonal to  $U |\psi\rangle$  and to  $A_j U |\psi\rangle, B_j U |\psi\rangle, C_j U |\psi\rangle$  for  $k \in \{l, l'\}, j \notin \{l, l'\}$ . Since  $U$  is unitary, we have that  $U^\dagger A_k U |\psi\rangle, U^\dagger B_k U |\psi\rangle, U^\dagger C_k U |\psi\rangle$  are orthogonal to  $U^\dagger U |\psi\rangle = |\psi\rangle$  and to  $U^\dagger A_j U |\psi\rangle, U^\dagger B_j U |\psi\rangle, U^\dagger C_j U |\psi\rangle$  for  $k \in \{l, l'\}, j \notin \{l, l'\}$ . Since the three vectors  $U^\dagger A_j U |\psi\rangle, U^\dagger B_j U |\psi\rangle, U^\dagger C_j U |\psi\rangle$  have the same span as  $A_j |\psi\rangle, B_j |\psi\rangle, C_j |\psi\rangle$  for all  $j$ , the proposition is established.  $\square$

## 7 Minimum Orbit Theorem

**Theorem 7.1.** *Minimum orbit dimension: For the local unitary group action on state space for  $n$  qubits, the smallest orbit dimension is*

$$\min\{\dim \mathcal{O}_x : x \in \mathbb{P}(H)\} = \begin{cases} \frac{3n}{2} & n \text{ even} \\ \frac{3n+1}{2} & n \text{ odd} \end{cases}.$$

We begin the proof by exhibiting a state for which the claimed minimum dimension is realized.

Let  $|s\rangle = |01\rangle - |10\rangle$  be a Hilbert space representative of the singlet state, let  $X = \begin{bmatrix} it & u \\ -\bar{u} & -it \end{bmatrix}$  be an element of  $\mathfrak{su}(2)$ . We have

$$(X, X) \cdot |s\rangle = 0$$

so  $(X, X)$  is in the isotropy Lie algebra of the state represented by  $|s\rangle$ .

From this it follows that  $(X_1, X_1, X_2, X_2, \dots, X_k, X_k)$  stabilizes the  $2k$ -qubit state  $x$  represented by  $\underbrace{|s\rangle \otimes |s\rangle \otimes \dots \otimes |s\rangle}_{k \text{ copies}}$  for all  $X_1, X_2, \dots, X_k$  in  $\mathfrak{su}(2)$ . Therefore  $LI_x$  has dimension at least  $3k = 3n/2$  for  $n = 2k$ , and therefore  $\dim \mathcal{O}_x \leq 3n - 3n/2 = 3n/2$  for  $n$  even.

Observe that  $(X_1, X_1, X_2, X_2, \dots, X_k, X_k, \begin{bmatrix} it & 0 \\ 0 & -it \end{bmatrix})$  stabilizes the  $(2k + 1)$ -qubit state  $x$  represented by  $|s\rangle \otimes |s\rangle \otimes \dots \otimes |s\rangle \otimes |0\rangle$  (by a phase factor), so the dimension of  $LI_x$  is at least  $3k + 1 = (3n - 1)/2$  for  $n = 2k + 1$ , and therefore  $\dim \mathcal{O}_x \leq 3n - (3n - 1)/2 = (3n + 1)/2$  for  $n$  odd.

These calculations establish that

$$\min\{\dim \mathcal{O}_x : x \in \mathbb{P}(H)\} \leq \begin{cases} \frac{3n}{2} & n \text{ even} \\ \frac{3n+1}{2} & n \text{ odd} \end{cases}. \quad (17)$$

Next we show that this bound on orbit dimension is sharp by establishing a lower bound for the rank of  $M$ . From 7.2 below, the desired lower bound for the minimum orbit dimension follows immediately from 3.3.

**Proposition 7.2.** *Minimum rank of  $M$ : Let  $x$  be a state for a system of  $n$  qubits, let  $|\psi\rangle$  be a Hilbert space representative for  $x$ , and let  $M$  be the real matrix associated to  $|\psi\rangle$  as defined in §3. We have*

$$\text{rank } M \geq \begin{cases} \frac{3n}{2} + 1 & n \text{ even} \\ \frac{3n+1}{2} + 1 & n \text{ odd} \end{cases}.$$

PROOF. Let  $\mathcal{C} = \{A_1|\psi\rangle, B_1|\psi\rangle, C_1|\psi\rangle, \dots, A_n|\psi\rangle, B_n|\psi\rangle, C_n|\psi\rangle, -i|\psi\rangle\}$  denote the set of columns of  $M$ . For a subset  $\mathcal{S} \subseteq \mathcal{C}$ , let  $\langle \mathcal{S} \rangle$  denote the real span of the column vectors contained in  $\mathcal{S}$ . Let  $\mathcal{S}_0$  be a subset of  $\mathcal{C}$  which is the union of some number  $p$  of triples, and is maximal with respect to the property that  $\langle \mathcal{S}_0 \rangle$  contains a subspace  $W$  for which

$$(i) \dim W \geq \begin{cases} \frac{3p}{2} & p \text{ even} \\ \frac{3p+1}{2} & p \text{ odd} \end{cases}, \quad \text{and}$$

$$(ii) W \perp \langle \mathcal{C} \setminus \mathcal{S}_0 \rangle.$$

We separate the argument into cases. We show that in every case, either 7.2 holds or we can derive a contradiction by constructing a superset  $\mathcal{S}_1$  of  $\mathcal{S}_0$  which is the union of some number  $p' > p$  of triples and which contains a subspace  $W'$  satisfying properties (i) and (ii) with  $p'$  in place of  $p$ . The construction of  $\mathcal{S}_1$  violates the maximality of  $\mathcal{S}_0$  and therefore rules out the case in question.

Case 1: Suppose that  $p = n$ , so that  $\mathcal{C} \setminus \mathcal{S}_0 = \{-i|\psi\rangle\}$ . Then property (ii) guarantees that  $\text{rank } M \geq \dim W + 1$ , so property (i) guarantees that 7.2 holds.

Case 2: Suppose that  $p < n$  and that the remaining triples  $T_{j_1}, T_{j_2}, \dots, T_{j_{n-p}}$  in  $\mathcal{C} \setminus \mathcal{S}_0$  have the maximum possible span, that is,

$$\dim\langle T_{j_1}, T_{j_2}, \dots, T_{j_{n-p}} \rangle = 3(n-p).$$

Properties (i) and (ii) imply that

$$\begin{aligned} \text{rank } M &\geq \dim W + \dim\langle \mathcal{C} \setminus \mathcal{S}_0 \rangle \\ &\geq \frac{3p}{2} + 3(n-p) \\ &= \frac{6n-3p}{2} \\ &\geq \frac{6n-(3n-3)}{2} \quad (\text{since } p \leq n-1) \\ &= \frac{3n+3}{2} \\ &= \frac{3n+1}{2} + 1 \end{aligned}$$

and so 7.2 holds. Note that if  $p = n-1$ , the hypothesis of full span is met by 5.1. Therefore in the remaining cases we need only consider  $p \leq n-2$ .

Case 3: Suppose  $p \leq n-2$  and that there is a pair of triples  $T_l, T_{l'}$  in  $\mathcal{C} \setminus \mathcal{S}_0$  with  $1 \leq l < l' \leq n$  such that  $\dim\langle T_l, T_{l'} \rangle \leq 4$ . Let  $\mathcal{S}_1 = \mathcal{S}_0 \cup T_l \cup T_{l'}$ , let  $p' = p+2$ , and let  $W' = W \oplus \langle T_l \cup T_{l'} \rangle$ , where “ $\oplus$ ” denotes the orthogonal direct sum. That the sum is orthogonal is guaranteed by property (ii) for  $W$ . Proposition 6.2 implies that property (ii) also holds for the pair  $(\mathcal{S}_1, W')$  and that  $\dim W' \geq \dim W + 3$ . It follows that if  $p$  is even, so is  $p'$  and we have

$$\dim W' \geq \frac{3p}{2} + 3 = \frac{3p+6}{2} = \frac{3(p+2)}{2} = \frac{3p'}{2}$$

and similarly if  $p$  and  $p'$  are odd we have

$$\dim W' \geq \frac{3p+1}{2} + 3 = \frac{3p'+1}{2}$$

so  $(\mathcal{S}_1, W')$  satisfies property (i). Thus  $\mathcal{S}_1$  violates the maximality of  $\mathcal{S}_0$ , so we conclude that the hypothesis of case 3 is impossible.

Case 4: Suppose  $p \leq n-2$  and that there is a pair of triples  $T_l, T_{l'}$  in  $\mathcal{C} \setminus \mathcal{S}_0$  with  $1 \leq l < l' \leq n$  such that  $\dim\langle T_l, T_{l'} \rangle = 5$ . Applying 6.1 we have four



vectors

$$|\zeta_l\rangle, |\eta_l\rangle \in \langle T_l \rangle, \quad |\zeta_{l'}\rangle, |\eta_{l'}\rangle \in \langle T_{l'} \rangle$$

which must span at least three dimensions, so once again  $\mathcal{S}_1 = \mathcal{S}_0 \cup T_l \cup T_{l'}$  with the subspace

$$W' = W \oplus \langle |\zeta_l\rangle, |\eta_l\rangle, |\zeta_{l'}\rangle, |\eta_{l'}\rangle \rangle$$

violates the maximality of  $\mathcal{S}_0$ . We conclude that the hypothesis of case 4 is impossible.

Case 5: The only remaining possibility is that  $p \leq n - 3$ . Let  $\mathcal{T} = \{T_{j_1}, T_{j_2}, \dots, T_{j_m}\}$  be a set of triples in  $\mathcal{C} \setminus \mathcal{S}_0$  with  $m \geq 3$  minimal with respect to the property

$$\dim \langle T_{j_1}, T_{j_2}, \dots, T_{j_m} \rangle < 3m.$$

Applying 6.1 we have two vectors

$$|\zeta_k\rangle, |\eta_k\rangle \in \langle T_k \rangle$$

for each of the  $m' \geq 2$  elements  $k \in K$ . Let

$$\mathcal{S}_1 = \mathcal{S}_0 \cup \left( \bigcup_{k \in K} T_k \right),$$

let  $p' = p + m'$ , and let

$$W' = W \oplus \langle \{|\zeta_k\rangle, |\eta_k\rangle\}_{k \in K} \rangle.$$

Note that property (ii) holds for  $(\mathcal{S}_1, W')$ . If  $m' < m$ , then the  $2m'$  vectors in  $\{|\zeta_k\rangle, |\eta_k\rangle\}_{k \in K}$  are independent by the minimality of  $\mathcal{T}$ , so we have

$$\dim W' \geq \dim W + 2m' \geq \frac{3p}{2} + 2m' = \frac{3p' + m'}{2} \geq \frac{3p' + 1}{2}$$

so property (i) holds for  $(\mathcal{S}_1, W')$ , but this contradicts the maximality of  $\mathcal{S}_0$ . Finally, if  $m' = m$ , then  $m \geq 4$  (since  $m'$  is even) and at least  $2(m - 1)$  of the vectors in  $\{|\zeta_k\rangle, |\eta_k\rangle\}_{k \in K}$  must be independent, again by the minimality of  $\mathcal{T}$ . If  $p$  is even, then  $p' = p + m$  is also even and we have

$$\dim W' \geq \dim W + 2(m - 1) \geq \frac{3p}{2} + 2(m - 1) = \frac{3p' + m - 4}{2} \geq \frac{3p'}{2}.$$

If  $p$  is odd, then  $p' = p + m$  is odd and we have

$$\dim W' \geq \dim W + 2(m - 1) \geq \frac{3p + 1}{2} + 2(m - 1) = \frac{3p' + m - 3}{2} \geq \frac{3p' + 1}{2}.$$

Thus  $\mathcal{S}_1$  with the subspace  $W'$  violates the maximality of  $\mathcal{S}_0$ . We conclude that the hypothesis of case 5 is impossible.

Having exhausted all possible cases, this completes the proof of 7.2, and hence of Theorem 7.1.  $\square$

## Acknowledgments

We are grateful for funding support from Lebanon Valley College for the initiation of this project in 2002–2003. S.N.W. thanks the Research Corporation for their support.

## References

- [1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [2] Stan Gudder. Quantum computation. *Amer. Math. Monthly*, 110(3):181–201, 2003.
- [3] Eric M. Rains. Polynomial invariants of quantum codes. *IEEE Trans. Inf. Theory*, 46:54–59, 2000. e-print quant-ph/9704042.
- [4] Markus Grassl, Martin Rötteler, and Thomas Beth. Computing local invariants of quantum-bit systems. *Phys. Rev. A*, 58:1833–1839, 1998. e-print quant-ph/9712040.
- [5] Anthony Sudbery. On local invariants of pure three-qubit states. *J. Phys. A*, 34:643–652, 2001. e-print quant-ph/0001116.
- [6] Yuriy Makhlin. Nonlocal properties of two-qubit gates and mixed states and optimization of quantum computations. *Quant. Info. Comput.*, 1:243–252, 2002. e-print quant-ph/0002045.
- [7] David A. Meyer and Nolan Wallach. *Invariants for multiple qubits: the case of 3 qubits*, chapter 3, pages 77–97. In Brylinski and Chen [9], 2002.
- [8] Jean-Luc Brylinski and Ranee Brylinski. *Invariant polynomial functions on  $k$  qudits*, chapter 11, pages 277–286. In Brylinski and Chen [9], 2002. e-print quant-ph/0010101.
- [9] Ranee K. Brylinski and Goong Chen, editors. *Mathematics of Quantum Computation*. Chapman & Hall/CRC, 2002.
- [10] David A. Meyer and Nolan R. Wallach. Global entanglement in multiparticle systems. Unpublished. e-print quant-ph/0108104.
- [11] Sergio Albeverio, Shao-Ming Fei, Preeti Parashar, and Wen-Li Yang. Non-local properties and local invariants for bipartite systems. *Phys. Rev. A*, 68:010303(R), 2003. e-print quant-ph/0307164.
- [12] M. S. Leifer, N. Linden, and A. Winter. Measuring polynomial invariants of multiparty quantum states. *Phys. Rev. A*, 69:052304, 2004. e-print quant-ph/0308008.

- [13] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach. Generalized Schmidt decomposition and classification of three-quantum-bit states. *Phys. Rev. Lett.*, 85:1560, 2000. e-print quant-ph/0003050.
- [14] A. Acín, A. Andrianov, E. Jané, and R. Tarrach. Three-qubit pure-state canonical forms. *J. Phys. A*, 34:6725, 2001. e-print quant-ph/0009107.
- [15] N. Linden and S. Popescu. On multi-particle entanglement. *Fortschr. Phys.*, 46:567–578, 1998. e-print quant-ph/9711016.
- [16] N. Linden, S. Popescu, and A. Sudbery. Non-local properties of multi-particle density matrices. *Phys. Rev. Lett.*, 83:243–247, 1999. e-print quant-ph/9801076.
- [17] D. Lyons and S. N. Walck. Generic orbit for local unitary action on  $n$ -qubit pure states. Unpublished.
- [18] H. A. Carteret and A. Sudbery. Local symmetry properties of pure 3-qubit states. *J. Phys. A*, 33:4981–5002, 2000. e-print quant-ph/0001091.
- [19] Marek Kuś and Karol Życzkowski. Geometry of entangled states. *Phys. Rev. A*, 63:032307, 2001. e-print quant-ph/0006068.
- [20] Magdalena M. Sinołęcka, Karol Życzkowski, and Marek Kuś. Manifolds of equal entanglement for composite quantum systems. *Acta Physica Polonica B*, 33:2081, 2002. e-print quant-ph/0110082.